Remarks

A new set of formal drawings is submitted to overcome the objections to the original drawings.

Informalities in claims 2, 3 and 6 are rended moot by the cancellation of these claims.

Multi-dependencies of claims 14-15 are also rended moot by the cancellation of these claims.

Multi-dependency of claim 16 is removed by amendment.

All claims 1-16 are rejected under 35 USC 102(e) as anticipated by Geiger (US 6,463,534). This rejection is rendered moot with respect to claims 1-6, 8, 10-11, and 14-15 by their cancellation. The rejection is respectfully traversed with respect to the remaining claims as amended.

Geiger is concerned with the problem of conducting secure transactions using security tokens such as smart cards. This is made clear in his summary of the invention. Applicants, on the other hand, are concerned with the problem of storing or replacing a user certificate in a security token in a way that guarantees that the user certificate is authenticated. The claimed invention describes a method to securely create new key pairs on the smart card and the storing of only valid certificates from an authority, designated by the root key/certificate during the issuing process of the security token and, further,

with the generation of a user certificate digital signature.

In the original specification, for example, see the last paragraph of page 2, the objective at the top of page 4 and the verification routing that is described on page 8.

The amended claims recite the purpose of verifying the storage of a user certificate in a security token. Amended claim7, for example, includes the steps of

> c) storing a verification component into said security token allowing use or replacement of a user certificate only when said user certificate is authenticated by said root certificate

and

> e) verifying a digital signature of the certification authority stored in the security token using a public root key of the certification authority.

Geiger does not teach or suggest the combination of these steps. In Geiger, a token authenticates itself to an attribute authority using the certificates that a pre-loaded into the token. The token, or device associated with the token, is then able to receive a resource from the attribute authority. But Geiger does not disclose a technique for verifying the storage of certificates in the token in the first or a later instance.

Claim 9 contains more specific details of the verification process, including the generation and matching of a hash value generated over a user certificate with a hash value that is stored in the user certificate. Geiger

does not describe any similar steps that are related to the storing of the user certificate in the token.

Independent claims 13 and 16 contain language similar to claim 9.

In view of the amendments and differences summarized above between the claims and Geiger, it is urged that the claims are in condition for allowance. Passage to issue is respectfully requested.

Respectfully Submitted,

Jerry W. Herndon
Attorney for Applicant
Reg. No. 27,901

Docket No. DE920000056US1
Customer No. 25259
Phone: 919-543-3754
Fax: 919-254-4330
Email: herndonj@us.ibm.com